REMARKS

Submitted herewith is a petition to extend the time for response from 13 October 2005 to 13 December 2005.

As a result of this amendment, the claims now pending in this application are claims 4, 11 - 13, 16, 20, and 22-34.

Claims 4, 11-13, 15, 20 and 22-28 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Nissl et al. in view of Pinizzotto. Applicants request reconsideration of those claims on the basis of the foregoing amendments considered together with the fact that neither of those references discloses or suggests Applicants' invention and there is no teaching in either reference that makes it obvious to modify the method or system of one with the teachings of the other so as to provide a method as defined by Applicants' claims.

Applicants' invention consists of modifying credit card transaction protocol to enhance security against fraud. As noted on page 1 of the application, in the section labeled "Background of the Invention", the information required to initiate a typical credit card transaction consists of a credit card number, an expiration date and the card holder's name and billing address. Applicants' invention reduces the risk of credit card fraud by generating a unique encrypted time-limited number that is based on a user's valid credit card information and may be used in completing a credit card transaction. Essentially that unique number functions as a time-limited credit card number that a third party vendor can submit for verification by the credit card issuer or a party authorized by the credit card issuer. Applicants' method also can be used for transactions where no third party vendor is involved, e.g., notably in direct transactions with a bank or other entity that is also the credit card issuer.

Applicants' invention involves generating a time-limited personal identification number (the "e-PIN" described in Applicants' specification (pages

3, lines 22-25 and page 8, lines 8-26) comprising in encrypted form a date/time stamp and certain information identifying the credit card user, and using that time-limited personal identification number to identify the credit card user in a proposed transaction. The time-limited personal identification number is transmitted to the credit card issuer, or a validating party authorized by the credit card issuer, and, at least in the case where a third party vendor is involved, transmittal of the time-limited personal identification number is accomplished via the vendor and is accompanied by other transaction information provided by the user.

The validation process involves (1) decrypting the time-limited credit card number, e.g., the ePIN, (2) determining the validity of the decrypted information by comparing it to information previously recorded by the credit card issuer or the authorized validating party and also determining from the decrypted date/time stamp whether the proposed transaction is within a predetermined time limit known to the validating party, and (3) communicating validation or rejection of the proposed credit card transaction to the vendor and/or the party initiating the proposed transaction on the basis of the acceptability of the decrypted time stamp and decrypted credit card information.

In addition to the novel concept of using a time-limited personal identification number to carry out a credit card transaction, Applicants' invention also is unique in two other respects:

(1) the time-limited personal identification number is generated using software provided by the credit card issuer (see page 2, lines 22-24; page 5, lines 6-10) of Applicant's application); and

(2) generation of the time-limited personal identification number may be accomplished without requiring interaction with any other party.

Thus in the case where the number-generating software is installed on the credit card user's own computer, the credit card user does not need to be connected to the third party vendor (if one is involved) or the credit card issuer

(or a party authorized by said credit card issuer to validate credit card transactions) in order to generate the time-limited personal identification number. Instead that time-limited number is generated off-line (see description on pages 5 and 8 of the application of howl, according to a preferred form of practicing the invention, a credit card user accesses a software program provided by the credit card issuer and previously installed on the user's computer to generate the time-limited personal identification number and to initiate a credit card transaction).

Applicants' invention offers a number of advantages and variations as follows:

(1) the time-limited personal identification number serves to limit the useful life of transaction information (see the sentence bridging pages 1 and 21 of the application), and thus provides security for credit card transactions;

(2) it offers the advantage of flexibility as well as security, with flexibility being achieved by virtue of the fact that the period of time during which the unique time-limited card number will be accepted for a proposed credit card transaction can be varied, and security being enhanced because if that unique credit card number is stolen from the vendor's database, no loss will ensue unless it is used within its predetermined lifetime;

(3) the invention is not limited to personal computers but can be practiced with other digital communication devices, e.g. a PDA, custom "smart card" device, or a cell phone;

(4) the credit card issuer may use a variety of encryption methods in the software used to generate the time-limited personal identification number, and

(5) the software used to generate the time-limited personal identification numbers need not be installed on the credit card user's personal computer or other digital communication device but may be installed on a remote server that is controlled by the credit card issuer or authorized validating party and is accessed by the credit card user (but not the third party vendor) using a

computer program and/or information provided by the credit card issuer or authorized validating party.

Another obvious advantage (but not specifically recited in Applicant's specification) is that, regardless of whether the software for generating the time-limited personal identification number is installed on the credit card user's own computer or on a remote server, the credit card issuer can electronically void or limit access to that software. Still another advantage of the invention is that credit card issuers implementing Applicants' method may use different distinct and unique encryption methods appropriate to the level of security desired. A further advantage is that the unique encrypted time-limited number may be transmitted to a vendor orally via a telephone conversation or in face-to-face meeting with a vendor. In such case the institution or vendor receiving the encrypted credit card number for a transaction processes it as it would any other credit card transaction.

The claims now in the application all define a method consistent with the invention as described in the application and the foregoing discussion. Those claims are believed to define patentably over Nissl et al. and Pinizzotto, whether considered individually or collectively, for the following reasons.

Nissl et al. U.S. Patent No. 6,530,023 has nothing to do with credit card transactions. Instead, as stated in col. 2, lines 56-60, it pertains to a specific method for sealing digital data to protect it against unauthorized access or manipulation and which is adapted for use in stationary operation (PCs, etc.) as well as during transport (fax, etc.). It achieves this by encrypting the digital data (col. 3, line 5; col. 5, lines 13-18, 26-30) and incorporating in the data, during the encryption process, a date/time stamp and an authentication code, e.g., a signature (col. 3, lines 9-11). This encrypted data is then transmitted to a selected receiver. At the receiver end, the encrypted data remains blocked (i.e., sealed) and can be accessed in readable form only after it has been decrypted. The time comparison using the decrypted time stamp is made to determine if the retrieved data arrived at

the proper time in order to discern the likelihood that the date had been manipulated. However, data manipulation is checked for by a parity check and other mathematical and/or hardware checking processes (col. 4, lines 36-40).

In contrast to the method disclosed by Nissl et al., Applicants' method has a gate-keeper function in the sense that after decryption of the time-limited personal identification number, the decrypting party not only (a) compares the decrypted credit card information with previously recorded information, and (b) makes a determination of the validity of the decrypted credit card information, but (c) also communicates that determination to the third party vendor, whereby the proposed transaction will proceed or not proceed, according to that communicated determination.

Pinizzotto patent application 20030097343 discloses a secured purchase card transaction system for conducting purchases over the Internet. The patented system comprises a plurality of customer encryption terminals 10, a plurality of merchant stations 12, and a processing center intervening between the customer (user) terminals and the merchant (vendor) stations. Each of the customer encryption terminals comprises a card swipe device for entering the credit card number, also a keyboard or the like to enter an identification number (PIN), and an encryption module which encrypts the credit card number as well as the PIN. That information, together with the customer ordering information (Par. 0006 of the patent) is sent over the Internet to the processing center which either rejects the credit card information or verifies that it is valid and sends a report, including customer ordering information, to the station 12 of the merchant targeted by the purchase request (Par. 0007).

The Pinizzotto system is similar to Applicants' in that the credit card number is encrypted so that the vendor does not have access to the customer's actual credit card number. However, it differs from Applicants' in that it uses a trusted agent as a transaction intermediary. Such systems are

well known, as exemplified by U.S. Patent No. 5,703,949, issued Dec. 30, 1997 to Sholom S. Rosen for "Method for Establishing Secure Communications Among Processing Devices". In the Pinizzotto system the user does not communicate directly with the vendor even with respect to the customer ordering information. In that respect, the Pinizzotto system differs from conventional credit card transactions where the customer deals directly with the merchant or other vendor.

Applicants' method differs from both the method employed by Pinizzotto and also the method involved in conventional credit card transactions involving direct communication between a credit card user and a third party vendor. In contrast to Pinizzotto, Applicants' method permits the credit card user to deal directly with a third party vendor. In contrast to conventional credit card transaction methods, Applicants' method does not require the credit card user to divulge his or her credit card number or other information known only to the user and the credit card issuer. The net result is that Applicants' method provides security while also permitting and facilitating direct dealing with a vendor. That result is achieved as a consequence of the step of generating an encrypted time-limited personal identification number as described, and then communicating that number directly to the vendor. Having an encrypted time-limited personal identification number allows the customer to provide that unique number to a vendor orally via phone or in face-to-face dealing for a proposed transaction, while still allowing the customer the option of conducting the transactions via the internet. The vendor receiving that encrypted time-limited number can confirm that number with the credit card issuer or other authorized validating entity as he would any other credit card number. **That is not possible using Pinizzotto's method**.

The rejection of Applicants' claims 4, 11 - 13, 16, 20, and 22-28 is premised on the Examiner's contention that since "..Nissl et al. teach the importance of financial transaction security.." and "...Pinizzotto teaches the importance of security for credit card transaction information..", it would "be

obvious to one with ordinary skill in the art to include [sic] credit card transaction encryption where the digital data is credit card data including PIN or PKN to the method of Nissl et al..". Applicant respectfully disagrees with that contention since **there is no suggestion in either Nissl et al. or Pinizzotto of using an encrypted time-limited personal identification number in a credit card transaction environment.** In the absence of such a suggestion, Applicants submit that the rejection based on the Examiner's use of the Nissl et al. and Pinizzotto references is not justified and should be withdrawn, particularly since the above-noted advantages of Applicants' method are lacking from both Nissl et al. and Pinizzotto and neither of them suggests that such advantages would result by modifying Nissl et al. in the manner suggested by the Examiner. Moreover, to modify Nissl et al. as suggested by the Examiner would create a system that in substance or purpose was never contemplated by Nissl et al. Additionally, in keeping with the scheme and the primary purpose of the Nissl et al. method, i.e., to prevent doctoring of data, all of the data involved in the credit card transaction would have to be encrypted, something that would frustrate direct dealing between a credit card user and a vendor, as permitted with Applicants' method.

To summarize, Applicants submit that modifying the Nissl et al. method to incorporate steps or procedures from the Pinizzotto method, or vice versa, is not obvious from either of those references and also would not result in a method corresponding in steps, purpose and advantages to the method defined by Applicants' claims, all of which relate to electronic credit card transactions and call for a an encrypted time-limited personal identification number (i.e., Applicants' ePIN) to be used to conduct a credit card transaction, with the vendor or other party to the proposed transaction, and the submittal of that time-limited number to the credit card issuer for validation.

It should be noted that the new claims submitted herewith differ only in scope from the other previously submitted claims that still remain in the application. Those new claims are submitted to assure proper coverage for

the invention. In this connection, it should be noted that dependent claims 32-34 are directed to use of the internet and/or a personal computer for conducting credit card transactions according to Applicants' invention.

In view of the foregoing remarks and the changes and additions to the claims, it is believed that this amendment places the application in condition for allowance. Therefore, prompt and favorable reconsideration is solicited.

Respectfully submitted,

12/5/05

Nicholas A. Pandiscio
Reg. No. 17,293
Pandiscio & Pandiscio
470 Totten Pond Road
Waltham, MA 02451-1914
Tel. (781) 290-0060
Fax (781) 290-4840

Mailing Certificate

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail, sufficient postage prepaid, in an envelope addressed to Mail Stop Amendment, Commissioner For Patents, P. O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below:

December 5, 2005
(date of deposit)

NICHOLAS A. PANDISCIO
(name of attorney)

(signature)

VASIL-1.AMB